PI 1154947

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

April 14, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: *60/442,486*
FILING DATE: *January 25, 2003*
RELATED PCT APPLICATION NUMBER: *PCT/US04/01845*

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

T. WALLACE
Certifying Officer

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

01-27-03

PTO/SB/18 (10-01)
Approved for use through10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. EU 359111336 US

INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Ronald L.	Rivest	Arlington, MA
Silvio	Micali	Brookline, MA

☒ Additional inventors are being named on the 1 separately numbered sheets attached hereto

TITLE OF THE INVENTION (500 characters max)

"Method and System for Micropayment Transactions"

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☐ Customer Number _____ → Place Customer Number Bar Code Label here

OR Type Customer Number here

☒ Firm or Individual Name	Perry Solomon, Peppercoin, Inc.				
Address	85 Central Street				
Address	Suite 205				
City	Waltham	State	MA	ZIP	02453
Country	USA	Telephone	781-891-8330	Fax	781-891-8386

ENCLOSED APPLICATION PARTS (check all that apply)

☒ Specification Number of Pages 11
☐ Drawing(s) Number of Sheets
☐ Application Data Sheet. See 37 CFR 1.76
☐ CD(s), Number
☐ Other (specify)

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant claims small entity status. See 37 CFR 1.27.
☐ A check or money order is enclosed to cover the filing fees
☐ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: _____
☒ Payment by credit card. Form PTO-2038 is attached.

FILING FEE AMOUNT ($)

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.
☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE _____

TYPED or PRINTED NAME Perry Solomon

TELEPHONE 781-891-8330, x14

Date 1/24/2003

REGISTRATION NO. (if appropriate)

Docket Number:

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

PROVISIONAL APPLICATION COVER SHEET
Additional Page

PTO/SB/16 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Docket Number	

INVENTOR(S)/APPLICANT(S)

Given Name (first and middle [if any])	Family or Surname	Residence (City and either State or Foreign Country)
Joseph	Bergeron	Cambridge, MA
Prasad	Jonnalagadda	Newton, MA
Perry	Solomon	Pawtucket, RI
Robert	Carney	Cambridge, MA

Number 1 of 1

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This document presents a preferred implementation of the Peppercoin protocol, as presented in PCT Application US02/12189, incorporated by reference. It is realized that many other implementations may exist.

Abstract:

An key benefit offered by Peppercoin, Inc. is payment-processing efficiency, yielding dramatically lower transaction processing costs. This paper describes one particular implementation of how that efficiency is engineered and a suggested implementation of Peppercoin's solutions.

Background:

In the "end of free" era of Internet content, consumers want pay-per-use options to complement subscription availability. Digital content owners recognize the enormous potential of pay-per-use models for items such as games, music, and software. Yet existing payment systems for low-value digital goods are characterized by high transaction costs, which in some cases exceed the value of the goods themselves. Fixed transaction fees constitute a significant barrier to profitability for low-priced transactions, and have inhibited the growth of vibrant markets for content priced below $1.00. Content owners are faced with the dilemma: How to provide consumers with flexible payment choices and still earn a profit?

Banks and payment processors levy a minimum transaction fee—usually at least $0.20—for every transaction, even those at very low price points.

Peppercoin has developed a revolutionary technology, as described in PCT Application US02/12189, incorporated by reference, that dramatically reduces the cost of processing low-value transactions. The new technology enables payments even lower than one cent without any form of subscription or pre-existing agreements between merchants and users. Peppercoin payments are a universal currency very much like cash: any one can pay one cent to someone else whenever he feels like, without any pre-established relationship, without even knowing the other person before hand, and without any promises of future transactions. As a result Peppercoin helps enable new markets for digital goods and services.

Document Methodology:

This document is a high-level overview of one particular implementation of how Peppercoin achieves dramatic advances in processing efficiencies to the immense benefit of Merchants and Consumers. It is not intended as a guide to deploying Peppercoin services or components, but rather to provide answers to the question "How does it work?"

This paper is structured by focusing on the requirements of each principal party within one preferred implementation of a Peppercoin enabled payment system **(Section I – Requirements)** and on the interplay among them **(Section II - Diagrams)**. It assumes familiarity with standard electronic commerce and Internet security practices and includes the use of such terms as digital certificates and digital signatures (see also Glossary of terms). It will explain why Peppercoin's system (as described in PCT Application US02/12189, incorporated by reference) is highly secure, safe, and fair to all participating parties. It will reveal the benefits to Merchants and Consumers but will not focus on these benefits (this topic is covered in other materials).

SECTION I—Requirements

There are four principal parties to consider in any payment system for digital goods or services.

Merchant—Party selling digital goods or services.

Consumer—Party purchasing digital goods or services.

Bank—A Bank generally plays one of two roles:

Acquiring Bank—Institution providing Merchant with an account for accepting payments.

Issuing Bank—Institution that maintains Consumer account for making payments. Bills Consumer for payments made to Merchants.

Payment Service Provider (PSP)—A third party that handles details—such as authentication, authorization, fraud detection—of acquiring and processing payment transactions between Merchants and Banks.

Certain functions may be undertaken by more than one party. For example, an Acquiring Bank may serve as payment processor, or those responsibilities may be undertaken by a third party. Payment Collection Services (PCS)—a set of functions discrete from payment settlement—are handled by the Merchant or by a third party service provider.

In the particular implementation of the Peppercoin payment scenario described in this paper, the **Peppercoin Payment Service** functions as the third party that handles both Payment Collection Services for the Merchant and performs Payment Processing (PSP) responsibilities. Note that in other deployment scenarios these activities may be fulfilled by other parties.

Merchant

■ Components Required in this particular implementation:

- **Peppercoin PSP account**
  In this particular implementation, a Merchant establishes an account with Peppercoin Payment Service to process payments.

- **Merchant bank account**
  In this particular implementation, a Merchant associates a bank account with the PSP (in this case, Peppercoin Payment Service) to receive the proceeds of purchases.

- **PepperMill software**
  In this particular implementation, Peppercoin provides an application called a PepperMill that the Merchant uses to prepare digital content for sale.

■ Actions Required to Sell Content in this particular implementation:

1. **Prepare Content to be Sold using PepperMill**
   a. The PepperMill converts a content file from its existing format to a *PepperBox format.* The resulting PepperBox file has a .PPB extension.
   For example, "Song.MP3" becomes → "Song.PPB"
   PepperBox Song.PPB contains information about Song.MP3—such as price and content description—as well as an encrypted version of the original Song.MP3 itself.
   b. The Merchant makes the PepperBox available to the Customer by posting it on a Website or via another file delivery method (e.g., email).

2. **Accept Peppercoins**
   a. Consumer downloads a PepperBox (e.g., Song.PPB) and uses PepperCoins as payment
   b. On Merchant's behalf (may alternatively be undertaken by Merchant), Peppercoin Payment Service accepts PepperCoins presented by authorized Consumer and sends the PepperBox decryption key to Consumer. Each PepperBox has a unique decryption key.
   On Merchant's behalf, Peppercoin Payment Service runs Peppercoin's automatic Selection Protocol, (as described in PCT Application US02/12189, incorporated by reference) to determine whether to submit PepperCoins for processing.*

3. **Receive payments from PSP**
   a. Peppercoin Payment Service deposits proceeds settled from Consumers to Merchant's bank account.

* The Selection process is discussed in the PSP subsection, as in this deployment scenario the PSP is undertaking the Merchant's Payment Collection (PCS) functions.

Consumer

■ Components Required in this particular implementation:

- **Peppercoin Consumer Account**
  In this particular implementation, Consumer establishes an account with Peppercoin Payment Service. This account can be pre- or post-paid by Consumer's payment instrument of choice.

- **Consumer Payment Instrument**
  Consumer uses an existing payment instrument– for example, a credit or charge card account—to be billed for PepperCoin payments.
- **PepperPanel software**
  Peppercoin will provide a small PepperPanel application that the Consumer uses to make PepperCoins and decrypt digital content.

■ Actions Required to Buy Content in this particular implementation:

1. **Download desired PepperBox**
   a. Consumer downloads PepperBox from Merchant Web site using browser or receives PepperBox as a file attachment (e.g., via email).
   b. Consumer opens PepperBox using PepperPanel, which displays content description and price.

2. **Purchase Content**
   a. Consumer purchases content using PepperPanel, which generates PepperCoins and sends to Merchant. Each PepperCoin contains information about the item being purchased as well as records the Consumer's cumulative spending. In this particular implementation, this information will be used later to bill the Consumer accurately.
   b. Merchant (or party performing Payment Collection Services—again, in this scenario Peppercoin Payment Service) accepts payment and sends decryption key to Consumer.

3. **Open Content**
   a. PepperPanel uses decryption key provided by Peppercoin Payment Service (on Merchant's behalf) to open content file.

4. **Pay Bill**
   a. Peppercoin Payment Service bills Consumer's Issuing Bank Account (Consumer designated payment instrument).

Bank

■ Components Required in this particular implementation:

- **None**

■ Actions Required in this particular implementation:

- **None**

In this particular implementation, the banking system requires no installed components or special actions to interface with the Peppercoin system unless bank chooses to function as a Payment Service Provider.

Peppercoin PSP

■ Components Required in this particular implementation:

- **PCS and Payment Processing software**
  Applications used for authentication, payment selection, and settlement.

■ Actions Required to Process Payments in this particular implementation:

1. **Receive Payments (on behalf of Merchant)**
   a. Validate PepperCoin presented by Consumer—check digital certificate, Consumer signature, expiration dates, whether Consumer is authorized to purchase this particular type of content, etc.
   b. Execute fraud detection procedures.

2. **Generate PepperBox Decryption Key (on behalf of Merchant)**
   a. Create unique decryption key for PepperBox and send to Consumer.

3. **Run Peppercoin Selection Protocol (on behalf of Merchant)**
   a. The core of Peppercoin's technology (as described in PCT Application US02/12189, incorporated by reference) is the process for sampling PepperCoins on a probabilistic basis. Some small percentage—say 1 in

100—of PepperCoins are chosen for processing in a manner that is secure, random, and non-controllable by the Consumer, Merchant, or PSP. The other PepperCoins not selected are never seen by the Bank (or Payment Service Provider) and thus not processed.

b. For those PepperCoins selected for processing, the Peppercoin protocol increases the value by a factor—say 100—that ensures the Merchant receives, on average, the value it should from all completed transactions.

For example, if all micropayments were 1 dime each, on average the merchant receives a single payment of $10 rather than 100 payments of $.10. While the cumulative incoming cash is the same, the single transaction cost for $10 payment is much preferable to 100 transaction costs for each of the one hundred $.10 payments.

4. **Process Selected PepperCoins**
   a. Peppercoin Payment Service validates PepperCoin—checks Consumer and Merchant digital certificates and signatures, expiration dates, whether Consumer is authorized to purchase the content, etc.
   b. Executes fraud detection procedures.
   c. Peppercoin Payment Service requests payment via the Consumer's payment instrument. The Consumer is billed for the cumulative amount spent using their individual Peppercoin account as indicated in the signed, selected PepperCoin (less previous amounts billed and settled).

5. **Pay Merchant**
   a. Peppercoin Payment Service deposits transaction proceeds (the selected PepperCoin increased in value by the factor specified by the protocol) in Merchant's bank account.

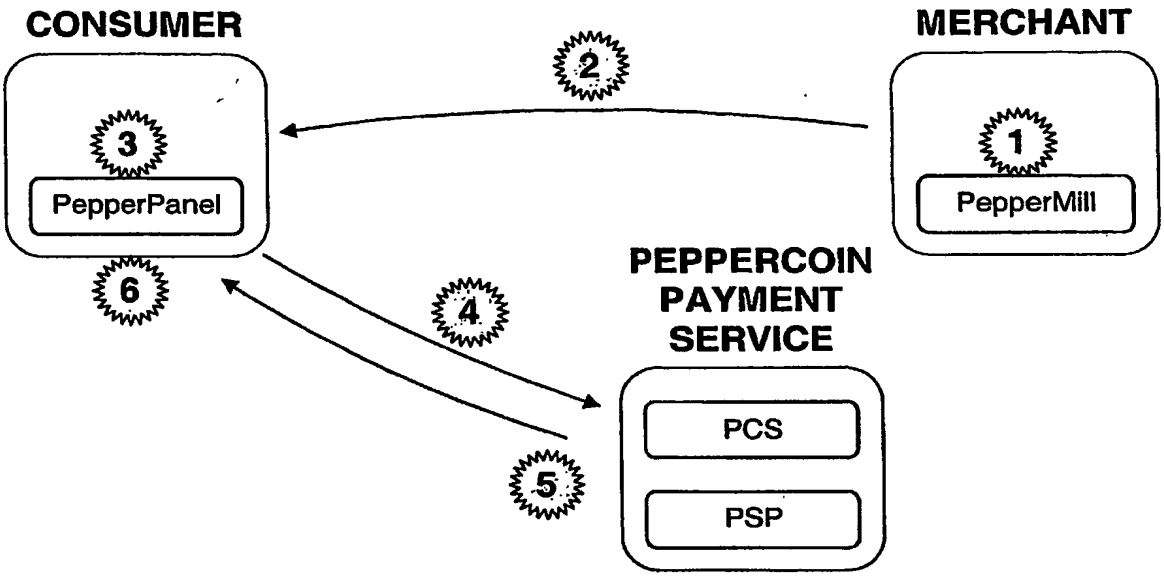
Summary

This section explained the requirements and processes that each principal party undertakes in the Peppercoin payment system in this particular implementation. The next section will illustrate how the parties interact.

The system provides for two primary interactions: A) the interaction between Consumer and Merchant; and B) the Payment Processing interaction.

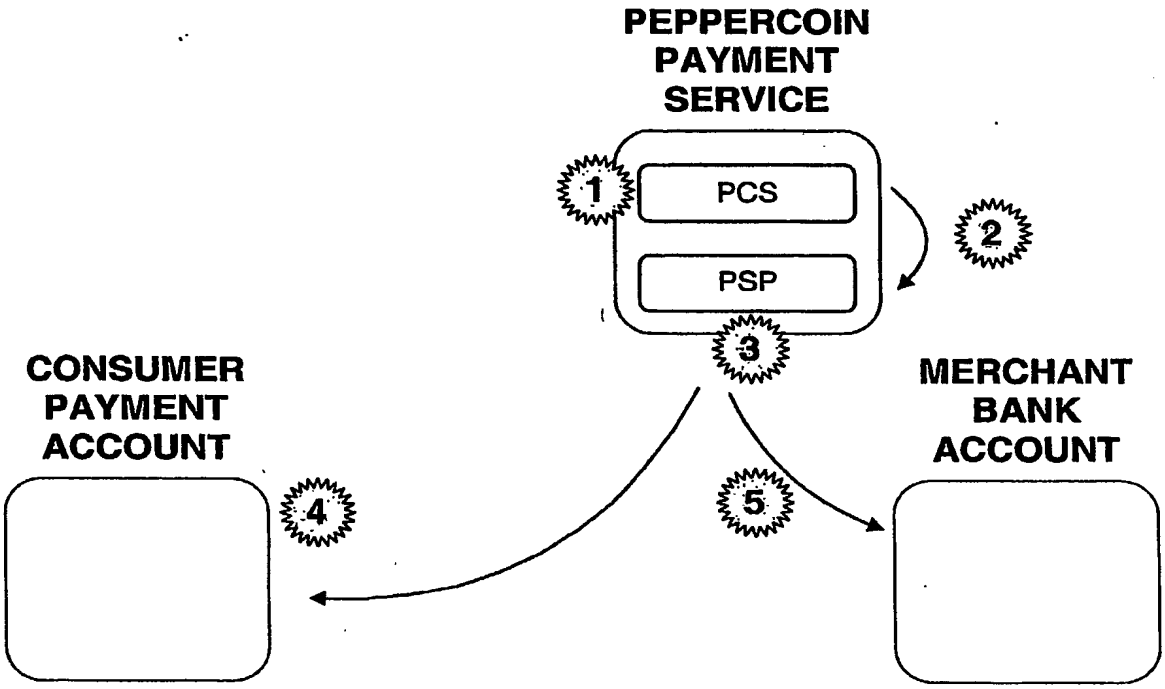
Section II
System Interplay

Diagram A: Consumer—Merchant Interaction



1. Merchant prepares content for sale. This process includes using PepperMill to produce PepperBox files.
2. Consumer downloads PepperBox file.
3. Consumer opens and views PepperBox file with the PepperPanel.
4. Consumer sends payment (in the form of a PepperCoin) to the PCS specified by the PepperBox. The PepperCoin contains Consumer's digital signature, the payment amount for that particular transaction, and cumulative payments made with Peppercoin Consumer Account.
   Note: PCS can be run by the Merchant itself or by a third party. In this scenario, Peppercoin Payment Service runs the PCS, but it can be thought of as a Merchant function.
5. PCS verifies payment validity and sends key to decrypt PepperBox to Consumer.
6. Consumer uses decryption key to open content.

Diagram B: Payment Processing Interaction



1. PCS runs payment selection protocol on the PepperCoin. In this example, 1 in 10 PepperCoins on average will be selected for processing.
2. PCS sends selected PepperCoin to PSP. Note this PepperCoin is "stepped up" to represent the total value the Merchant should, on average, receive for all Consumer transactions. The "step up" factor in this example is 10x.
3. PSP checks validity of selected PepperCoin (checks digital signatures and certificates of Consumer and Merchant PCS).
4. PSP settles payment with Consumer, i.e., Consumer is billed the cumulative amount that individual Consumer spent as indicated on the signed PepperCoin.
5. PSP settles payment with Merchant, i.e., Merchant receives the "stepped up" value represented by the selected PepperCoin.

Glossary

Authentication
The action of positively identifying the entity that sends a message.

Certificate
In cryptography, an electronic document binding some pieces of information together, such as a user's identity and public-key. They allow verification of the claim that a specific public key does in fact belong to a specific individual. Certificates help prevent someone from using a phony key to impersonate someone else. Certificate Authorities (CA's) provide certificates.

In their simplest form, certificates contain the digital signature of the certificate issuer.

Certificate Authority
An entity (typically a company) that issues digital certificates to other entities (organizations or individuals) to allow them to prove their identity to others. A Certificate Authority might be an external company, such as Peppercoin or VeriSign that offers digital certificate services or an internal organization such as a corporate MIS department. The Certificate Authority's chief function is to verify the identity of entities and issue digital certificates attesting to that identity.

Cipher
An encryption-decryption algorithm.

Ciphertext
Encrypted data.

Encryption
The transformation of plaintext into an apparently less readable form (called ciphertext) through a mathematical process. The ciphertext may be read by anyone.

Digital signature
A digital guarantee that a file has not been altered, as if it were carried in an electronically sealed envelope. The "signature" is an encrypted digest (one-way hash) of the message or other file. The recipient decrypts the digest that was sent and also recomputes the digest from the received file. If the digests match, the file is proved intact and tamper free from the sender.

Key
A string of bits used widely in cryptography, allowing people to encrypt and decrypt data; a key can be used to perform other mathematical operations as well. Given a cipher, a key determines the mapping of the plaintext to the ciphertext.

Key pair
The full key information in a public-key cryptosystem, consisting of the public key and private key.

Message digest
A condensed text string that has been distilled from the contents of a text message. Its value is derived using a one-way hash function (easy to compute but difficult to invert) and is used to create a digital signature.

PCS
Acronym for Payment Collection Services. The activities and functions related to the acceptance of payment. In the Peppercoin system, this includes validation of PepperCoins, fraud detection, and the PepperCoin selection process. Generally understood as a Merchant function, a distinction is made between payment collection and content preparation ("PepperMilling") because Merchants may choose to outsource the former to a third party.

PepperBox
A file encrypted by a PepperMill application. This file contains an encrypted underlying file or application (the "content"), a price tag for the content that includes currency and whom to pay, and a description of the content. PepperBox files have a .PPB name extension.

PepperCoin
The digital "checks" used in the Peppercoin payment system. PepperCoins represent genuine currency (money), and are unique to—and signed by—an individual Consumer, just as in a regular checking account.

Peppercoin, Inc.
A private corporation that offers highly efficient payment technology and services.

PepperMill
The Merchant content preparation application in the Peppercoin system. Used to package and encrypt digital goods for sale.

PepperPanel
The Consumer application in the Peppercoin system. Used to create PepperCoins, manage Peppercoin accounts, and manage and decrypt PepperBox files.

Private key
In public-key cryptography, this key is the secret key. It is primarily used for decryption but is also used to create digital signatures.

Public key
In public-key cryptography this key is made public to all, it is primarily used for encryption but can be used for verifying signatures.

Public-key cryptography
An encryption scheme where each person gets a pair of keys, called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his private key. The need for sender and receiver to share secret information (keys) via some secure channel is eliminated: all communications involve only public keys, and no private key is ever transmitted or shared.